

# Improved Deterministic $N$ -To-One Joint Remote Preparation of an Arbitrary Qubit via EPR Pairs

Wen-Jie Liu · Zheng-Fei Chen · Chao Liu · Yu Zheng

Received: date / Accepted: date

**Abstract** Recently, Bich et al. (Int. J. Theor. Phys. 51: 2272, 2012) proposed two deterministic joint remote state preparation (JRSP) protocols of an arbitrary single-qubit state: one is for two preparers to remotely prepare for a receiver by using two Einstein-Podolsky-Rosen (ERP) pairs; the other is its generalized form in the case of arbitrary  $N$  ( $N > 2$ ) preparers via  $N$  ERP pairs. While examining these two protocols, we find that the success probability for the receiver achieving the desired state is not deterministic, i.e.,  $P_{suc}^{N>2} < 1$ , for  $N > 2$  preparers in the second protocol. Through constructing two sets of adaptive projective measurement bases for both the real space and the complex space, an improved deterministic  $N$ -to-one JRSP protocol for an arbitrary single-qubit state is presented. Analysis shows our protocol can truly achieve the unit success probability, i.e.,  $P_{suc}^{N\geq 2} = 1$ . What is more, the receiver can be randomly assigned even after the distribution of the qubits of EPR pairs, so it is more flexible and applicable in the network situation.

**Keywords** Joint remote state preparation ·  $N$ -to-one · EPR pairs · Projective measurement basis · Unit success probability

## 1 Introduction

With the rapid development of quantum mechanics in recent decades, many protocols of quantum information have been flourished by utilizing quantum

---

W.-J. Liu · Y. Zheng  
Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing 210044, P.R.China  
E-mail: wenjiel@163.com

W.-J. Liu · Z.-F. Chen · C. Liu · Y. Zheng  
School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, P.R.China

mechanics principles, including quantum key distribution (QKD) [1-3], quantum secret sharing (QSS) [4-6], quantum direct communication (QDC) [7-9], quantum teleportation (QT) [10-12], quantum private comparison (QPC) [13-15], and so on. In the recent ten years, a new direction, remote state preparation (RSP) [16-18], has become a hot topic in the quantum information field. Similar to QT, in RSP the preparer can exploit the nonlocal correlation of the quantum entangled state shared in advance to prepare the original state in the remote place. But the main difference is that the preparer must know all the information of the state in RSP, while in QT the preparer knows nothing about the state.

The early RSP protocols always focus on one preparer and one receiver, and the preparer knows all the information of the prepared state. However, for some highly sensitive and important information, it might be unreliable to let one preparer hold everything. To overcome this defection, joint remote state preparation (JRSP) was put forward. The pioneering JRSP protocol was proposed by Xia et al. [19] in 2007, in which the authors realize the multiparty remote preparation of the quantum state  $(\alpha|0\rangle^{\otimes M} + \beta|1\rangle^{\otimes M})$ ,  $M = 1, 2, \dots, \infty$  with unit fidelity but less than unit probability between  $N - 1$  senders and one receiver using one  $N$ -particle non-maximally entangled Greenberger-Horne-Zeilinger (GHZ) state as the quantum channel. Since then, JRSP has attracted a lot of attention in recent years [20-25]. Unfortunately, these protocols are probabilistic, i.e., they cannot be realized with unit success probability.

To ensure the unit success probability of JRSP, a new direction of JRSP, namely deterministic JRSP, has been put forward. In 2011, Xiao et al. [26] introduced a three-step strategy of JRSP to remotely prepare an arbitrary two- and three-qubit state by using GHZ states as the shared quantum resource. In this protocol, two preparers measure their qubits orderly rather than independently, and the success probability of preparation can be increased to 1. Inspired by the three-step strategy, many other deterministic JRSP protocols have been proposed [27-30]. For example, In 2012, An et al. [27] put forward a scheme to deterministically prepare the most general single- and two-qubit state by using four Einstein-Podolsky-Rosen (EPR) pairs as the shared quantum resource. And then, Chen et al. [28] proposed a scheme to joint remotely prepare an arbitrary three-qubit state deterministically by using six EPR pairs. In 2013, Wang et al. [29] proposed a scheme to jointly and remotely prepare an arbitrary two-qubit state, and generalize it to the arbitrary three-qubit case. Compared with Refs. [27] and [28], Wang et al.'s protocol just requires two EPR pairs and one GHZ state in the arbitrary two-qubit case and four EPR pairs and one GHZ states in the arbitrary three-qubit case. Being more robust and persistent than GHZ states, Cluster states are also utilized in JRSP. In 2013, Wang et al. [30] proposed a new version of deterministic JRSP protocol for an arbitrary two-qubit state by using the six-qubit cluster state. However, To the authors knowledge, most of deterministic JRSP protocols only focus on the two-preparer case, and these protocols are impossible or difficult to be directly generalized to the arbitrary preparers case.

Recently, Bich et al. [31] proposed two deterministic JRSP protocols using ERP pairs: one is for two preparers to remotely prepare arbitrary single-qubit state; and the other is for  $N$  ( $N > 2$ ) preparers. The authors claim that the total success probability is 1 ( $P_{suc} = 1$ ) both for two preparers and  $N > 2$  preparers. Unfortunately, we find it is not true in case of  $N > 2$  preparers: the success probability  $P_{suc}^{N>2} < 1$ . In order to solve the problem, we tactfully constructed two sets of projective measurement bases, i.e., the real-coefficient measurement basis and the complex-coefficient measurement basis, and further proposed an  $N$ -to-one JRSP protocol for an arbitrary single-qubit state with unit success probability (i.e,  $P_{suc}^{N\geq 2} = 1$ ).

The paper is organized as follows. In the next section, Bich et al.'s second protocols, especially the second protocol, are briefly reviewed and its correctness analysis is given in detail. In Sect. 3, two sets of projective measurement bases are constructed, and based on them, an improved deterministic  $N$ -to-one JRSP protocol of an arbitrary single-qubit state is proposed. Finally, a concise summary is rendered in Sect. 4.

## 2 Review of Bich et al.'s protocols and the correctness analysis

### 2.1 Review of Bich et al.'s protocols

In Bich et al.'s first protocol, they proposed a deterministic JRSP protocol with  $N = 2$  preparers and a receiver. In this protocol, two preparers, Alice and Bob, can help the remote receiver, Charlie, prepare a single-qubit state

$$|\phi\rangle = a|0\rangle + b^{i\varphi}|1\rangle, \quad (1)$$

where coefficients  $a, b$  are real with the normalization condition  $|a|^2 + |b|^2 = 1$ , and  $\varphi \in [0, 2\pi]$ . To our knowledge, the success probability for the receiver achieving the desired state is truly 1, so we just skip the detail of Bich et al.'s first protocol. In the appendix, Bich et al. propose the second protocol with  $N > 2$  preparers, in which the authors tried to directly generalize the first protocol to the situation of  $N > 2$  preparers, but unfortunately, there exists a fatal problem. Before reviewing the procedures of Bich et al.'s second protocol, we need have some knowledge about the pre-shared quantum channel among  $N$  preparers (Alice, Bob 1, Bob 2, ..., Bob  $N$ ) and a receiver (Charlie) as shown in Fig. 1.

For the convenience of description, the authors took  $N = 3$  (Alice, Bob 1, and Bob 2), and the participants pre-share three EPR pairs as the quantum channel

$$|Q\rangle_{A_1 B_1 A_2 B_2 A_3 C} = |EPR\rangle_{A_1 B_1} |EPR\rangle_{A_2 B_2} |EPR\rangle_{A_3 C}, \quad (2)$$

where  $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , qubits  $A_1, A_2, A_3$  are hold by Alice, and qubits  $B_1, B_2, C$  by Bob 1, Bob 2 and Charlie, respectively. Alice is allowed to know  $\{a, b\}$ , Bob 1 and Bob 2 share the knowledge of  $\varphi$  in the following

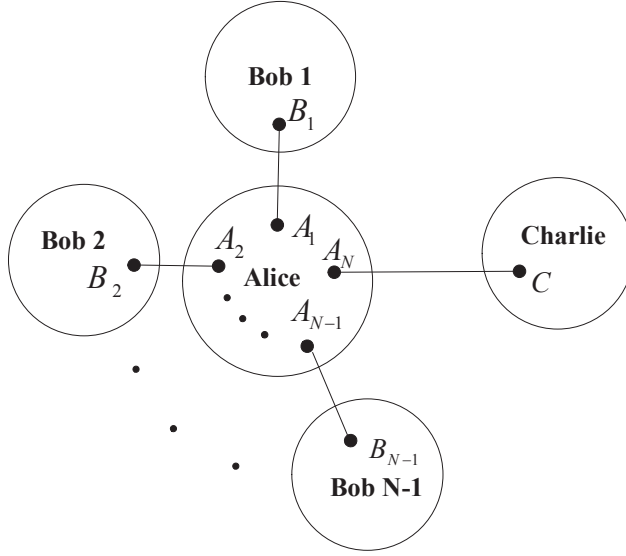


Fig. 1: <sup>[31]</sup> The qubits distribution for JRSP of the most general single-qubit state via  $N$  EPR pairs for the situation of  $N$  preparers (Alice, Bob 1, Bob 2, . . . and Bob N-1) and a receiver (Charlie). Qubits are represented by dots and entangled qubits are connected by a solid line.

way: Bob 1 knows  $\varphi_1$  and Bob 2 knows  $\varphi_2$ , and  $\varphi = \varphi_1 + \varphi_2$ . The detailed three-step protocol for  $N = 3$  preparers can be described as below.

**Step 1.** Alice measures her three qubits in the basis  $\{|u_{klm}\rangle_{A_1 A_2 A_3}; k, l, m \in \{0, 1\}\}$ ,

$$\begin{pmatrix} |u_{000}\rangle_{A_1 A_2 A_3} \\ |u_{001}\rangle_{A_1 A_2 A_3} \\ |u_{010}\rangle_{A_1 A_2 A_3} \\ |u_{011}\rangle_{A_1 A_2 A_3} \\ |u_{100}\rangle_{A_1 A_2 A_3} \\ |u_{101}\rangle_{A_1 A_2 A_3} \\ |u_{110}\rangle_{A_1 A_2 A_3} \\ |u_{111}\rangle_{A_1 A_2 A_3} \end{pmatrix} = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ b & 0 & 0 & 0 & 0 & 0 & 0 & -a \\ 0 & a & 0 & 0 & 0 & 0 & b & 0 \\ 0 & b & 0 & 0 & 0 & 0 & -a & 0 \\ 0 & 0 & a & 0 & 0 & b & 0 & 0 \\ 0 & 0 & b & 0 & 0 & -a & 0 & 0 \\ 0 & 0 & 0 & a & b & 0 & 0 & 0 \\ 0 & 0 & 0 & -b & a & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} |000\rangle_{A_1 A_2 A_3} \\ |001\rangle_{A_1 A_2 A_3} \\ |010\rangle_{A_1 A_2 A_3} \\ |011\rangle_{A_1 A_2 A_3} \\ |100\rangle_{A_1 A_2 A_3} \\ |101\rangle_{A_1 A_2 A_3} \\ |110\rangle_{A_1 A_2 A_3} \\ |111\rangle_{A_1 A_2 A_3} \end{pmatrix}, \quad (3)$$

and publicly broadcasts the measurement outcome to Bob 1, Bob 2 and Charlie. Expressing the quantum channel  $|Q\rangle_{A_1 B_1 A_2 B_2 A_3 C}$  through  $|u_{klm}\rangle_{A_1 A_2 A_3}$ ,

$$|Q\rangle_{A_1 B_1 A_2 B_2 A_3 C} = \frac{1}{2\sqrt{2}} \sum_{m=0}^1 \sum_{l=0}^1 \sum_{k=0}^1 |u_{klm}\rangle_{A_1 A_2 A_3} |L_{klm}\rangle_{B_1 B_2 C}, \quad (4)$$

we derive  $|L_{klm}\rangle_{B_1 B_2 C}$  in the form

$$|L_{000}\rangle_{B_1 B_2 C} = a|000\rangle_{B_1 B_2 C} + b|111\rangle_{B_1 B_2 C}, \quad (5)$$

$$|L_{001}\rangle_{B_1 B_2 C} = -a|111\rangle_{B_1 B_2 C} + b|000\rangle_{B_1 B_2 C}, \quad (6)$$

$$|L_{010}\rangle_{B_1 B_2 C} = a|001\rangle_{B_1 B_2 C} + b|110\rangle_{B_1 B_2 C}, \quad (7)$$

$$|L_{011}\rangle_{B_1 B_2 C} = -a|110\rangle_{B_1 B_2 C} + b|001\rangle_{B_1 B_2 C}, \quad (8)$$

$$|L_{100}\rangle_{B_1 B_2 C} = a|010\rangle_{B_1 B_2 C} + b|101\rangle_{B_1 B_2 C}, \quad (9)$$

$$|L_{101}\rangle_{B_1 B_2 C} = -a|101\rangle_{B_1 B_2 C} + b|010\rangle_{B_1 B_2 C}, \quad (10)$$

$$|L_{110}\rangle_{B_1 B_2 C} = a|011\rangle_{B_1 B_2 C} + b|100\rangle_{B_1 B_2 C}, \quad (11)$$

$$|L_{111}\rangle_{B_1 B_2 C} = a|100\rangle_{B_1 B_2 C} - b|011\rangle_{B_1 B_2 C}. \quad (12)$$

**Step 2.** Bob 1 and Bob 2 independently measure their qubits. If  $klm = 000$  or  $010$ , each Bob  $j$  ( $j = 1, 2$ ) uses a measurement basis determined by

$$\begin{pmatrix} |v_0\rangle_{B_j} \\ |v_1\rangle_{B_j} \end{pmatrix} = V^{(0)}(\varphi_j) \begin{pmatrix} |0\rangle_{B_j} \\ |1\rangle_{B_j} \end{pmatrix}; \quad (13)$$

If  $klm = 001$  or  $011$ , the basis for each Bob  $j$  is

$$\begin{pmatrix} |v_0\rangle_{B_j} \\ |v_1\rangle_{B_j} \end{pmatrix} = V^{(1)}(\varphi_j) \begin{pmatrix} |0\rangle_{B_j} \\ |1\rangle_{B_j} \end{pmatrix}, \quad (14)$$

where

$$V^{(r)}(\varphi) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-(-1)^r i\varphi} \\ e^{(-1)^r i\varphi} & -1 \end{pmatrix}, r \in \{0, 1\}. \quad (15)$$

In case  $klm = 100$  or  $110$ , Bob 1 uses a measurement basis determined by Eq.(13), and the basis for Bob 2 is Eq. (14); while  $klm = 101$  or  $111$ , the bases for Bob 1 and Bob 2 are determined by Eq. (14) and (13), respectively. After measurement, Bob 1 and Bob 2 announce their measurement outcomes  $n, s$  ( $n, s \in \{0, 1\}$ ) to Charlie.

**Step 3.** Charlie converts the qubit  $C$  to be the desired state  $|\phi\rangle_C$  by applying reconstruction operators  $R_{klmns}$ . The operators  $R_{klmns}$  that Charlie needs in this step are shown in Table 1.

Table 1: <sup>[31]</sup> The reconstruction operator  $R_{klmns}$ , conditioned on the measurement outcomes  $klm$ ,  $n$  and  $s$  of Alice, Bob 1 and Bob 2, respectively.

$I$  is the identity operator,  $X = |0\rangle\langle 1| + |1\rangle\langle 0|$  the bit-flip operator and  $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$  the phase-flip one

#	$klmns$	$R_{klmns}$
1-8	00000, 00011, 10000, 10011, 01101, 01110, 11101 or 11100	$I$
9-16	01000, 01011, 11000, 11011, 00101, 00110, 10101 or 10110	$X$
17-24	00100, 00111, 10100, 10111, 01001, 01010, 11001123 or 11010	$ZX$
25-32	01100, 01111, 11100, 11111, 00001, 00010, 10001 or 10010	$Z$

## 2.2 Correctness analysis

In Ref. [31], the authors claimed the receiver can get the desirable state with the unit success probability ( $P_{suc} = 1$ ) both for two preparers and  $N > 2$  preparers. In fact, it is not true in the case of  $N > 2$  preparers. In the following, we will analyze its correctness in detail.

In Step 1, Alice measures her three qubits in the basis  $\{|u_{klm}\rangle_{A_1 A_2 A_3}; k, l, m \in \{0, 1\}\}$  and publishes her outcome to the other participants (Bob 1, Bob 2 and Charlie). For sake of clearness, we assume the measurement outcome is  $klm = 010$ , and according to the selection strategy of measurement basis in Step 2, Bob 1 and Bob 2 will use the measurement basis of Equation (13), i.e., the basis for Bob 1 is  $\begin{pmatrix} |v_0\rangle_{B_1} \\ |v_1\rangle_{B_1} \end{pmatrix} = V^0(\varphi_1) \begin{pmatrix} |0\rangle_{B_1} \\ |1\rangle_{B_1} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi_1} \\ e^{i\varphi_1} & -1 \end{pmatrix} \begin{pmatrix} |0\rangle_{B_1} \\ |1\rangle_{B_1} \end{pmatrix}$ , and the basis for Bob 2 is  $\begin{pmatrix} |v_0\rangle_{B_2} \\ |v_1\rangle_{B_2} \end{pmatrix} = V^0(\varphi_2) \begin{pmatrix} |0\rangle_{B_2} \\ |1\rangle_{B_2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi_2} \\ e^{i\varphi_2} & -1 \end{pmatrix} \begin{pmatrix} |0\rangle_{B_2} \\ |1\rangle_{B_2} \end{pmatrix}$ . Then,  $|L_{010}\rangle_{B_1 B_2 C}$  can be rewritten as

$$\begin{aligned} |L_{010}\rangle_{B_1 B_2 C} &= \frac{1}{2} \sum_{n=0}^1 \sum_{s=0}^1 |v_n\rangle_{B_1} |v_s\rangle_{B_2} |\phi\rangle_C \\ &= \frac{1}{2} |v_0\rangle_{B_1} |v_0\rangle_{B_2} (a|1\rangle + be^{i(\varphi_1+\varphi_2)}|0\rangle)_C \\ &\quad + \frac{1}{2} |v_0\rangle_{B_1} |v_1\rangle_{B_2} (ae^{-i\varphi_2}|1\rangle - be^{i\varphi_1}|0\rangle)_C \\ &\quad + \frac{1}{2} |v_1\rangle_{B_1} |v_0\rangle_{B_2} (ae^{-i\varphi_1}|1\rangle - be^{i\varphi_2}|0\rangle)_C \\ &\quad + \frac{1}{2} |v_1\rangle_{B_1} |v_1\rangle_{B_2} (ae^{-i(\varphi_1+\varphi_2)}|1\rangle + b|0\rangle)_C. \end{aligned} \quad (16)$$

Obviously, only when  $ns = 00$ , qubit  $C$  will collapse into  $|\phi\rangle_C = a|1\rangle + be^{i(\varphi_1+\varphi_2)}|0\rangle$ , and the receiver can achieve the desirable state just with the identity operator. But if  $ns = 01$  ( $|\phi\rangle_C = ae^{-i\varphi_2}|1\rangle - be^{i\varphi_1}|0\rangle$ ),  $10$  ( $|\phi\rangle_C = ae^{-i\varphi_1}|1\rangle - be^{i\varphi_2}|0\rangle$ ) or  $11$  ( $|\phi\rangle_C = ae^{-i(\varphi_1+\varphi_2)}|1\rangle + b|0\rangle$ ), there is no any appropriate unitary operator that can be adopted to transform the state  $|\phi\rangle_C$  to the desirable state. That is to say, the probability for Charlie finding the desirable state is  $1/4$  under this situation.

In the general case, there are eight possible outcomes  $\{000, 001, 010, 011, 100, 101, 110, 111\}$  for Alice, and the probability of each outcome is equal. That means, the probability for Alice obtaining each state  $|u_{klm}\rangle_{A_1 A_2 A_3}$  ( $k, l, m = 0, 1$ ) is  $1/8$ . Similar to the case of  $klm = 010$ , Charlie can also obtain the desirable state with the probability of  $1/4$  in the other seven cases. So, the total success probability is

$$P_{suc}^{N=3} = \left(\frac{1}{8} \times \frac{1}{4}\right) \times 8 = \frac{1}{4} < 1. \quad (17)$$

Clearly, this is contrary to what the authors claimed: “the total success probability is obviously 1” [31].

### 3 Improved deterministic $N$ -to-one JRSP of an arbitrary qubit

#### 3.1 The construction of measurement basis

The construction of measurement basis is at the heart of RSP or JRSP, and it is the key point that will influence the final success probability of obtaining the desirable state. In order to improve the success probability of the  $N$ -to-one JRSP to 1, the first task is to tactfully construct two suitable sets of measurement bases, the real-coefficient measurement basis and the complex-coefficient one.

In our JRSP protocol, we will use the projective measurements to measure the qubits. Before constructing these ingenious projective measurement bases, we need have some knowledge of projective measurement.

**Theorem 1** *Projective measurement*<sup>[32]</sup>: A projective measurement is described by an observable,  $M$ , a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_m m P_m, \quad (18)$$

where  $P_m$  is the projector onto the eigenspace of  $M$  with eigenvalue  $m$ . The possible outcomes of the measurement correspond to the eigenvalues,  $m$ , of the observable.

According to the definition of projective measurement (Theorem 1), projective measurement can be understood as a special case of Postulate 3 (i.e., the quantum measurement postulate, seen in Refs. [32] and [33]). Specifically, a complete set of orthogonal projectors  $P_m$  satisfy the following relations: (1)  $\sum_m P_m = I$ ; and (2)  $P_m P_{m'} = \delta_{m,m'} P_m$  ( $\delta_{m,m'} = 1$ , if  $m = m'$ ;  $\delta_{m,m'} = 0$ , if  $m \neq m'$ ). In quantum information field, a widely used phrase, to ‘measure in a basis  $|m\rangle$ ’, where  $|m\rangle$  form an orthonormal basis, simply means to perform the projective measurement with projectors as below

$$P_m = |m\rangle \langle m|. \quad (19)$$

In our protocol, Alice holds  $N$  qubits  $A_1, A_2, \dots, A_N$ , and she knows the real part  $\{a, b\}$  of the state (given in Eq. (1)). So the projection operators  $\{P_m\}$  can be described as  $P_m = |u_{l_1, l_2, \dots, l_N}\rangle_{A_1, A_2, \dots, A_N} \langle u_{l_1, l_2, \dots, l_N}|_{A_1, A_2, \dots, A_N}$  ( $l_1, l_2, \dots, l_N \in \{0, 1\}$ ), where the set of states  $\{|u_{l_1, l_2, \dots, l_N}\rangle_{A_1, A_2, \dots, A_N}\}$  is a complete set of orthonormal basis and can be defined as

$$\begin{pmatrix} |u_{00\dots 0}\rangle \\ |u_{00\dots 1}\rangle \\ \vdots \\ |u_{11\dots 0}\rangle \\ |u_{11\dots 1}\rangle \end{pmatrix} = \begin{pmatrix} a & 0 & \cdots & 0 & b \\ 0 & a & & b & 0 \\ & & \ddots & & \\ & \vdots & & a & b \\ & & & -b & a \\ & & & & \vdots \\ 0 & -b & \cdots & a & 0 \\ -b & 0 & & 0 & a \end{pmatrix} \begin{pmatrix} |00\dots 0\rangle \\ |00\dots 1\rangle \\ \vdots \\ |11\dots 0\rangle \\ |11\dots 1\rangle \end{pmatrix}. \quad (20)$$

The Eq. (20) can be generalized to a collection  $\{|u_{l_1 l_2 \dots l_N}\rangle = a|l_1 l_2 \dots l_N\rangle_{A_1, A_2, \dots, A_N} + (-1)^{l_1} b|\bar{l}_1 \bar{l}_2 \dots \bar{l}_N\rangle_{A_1, A_2, \dots, A_N} \mid l_k \in \{0, 1\}, \bar{l}_k = 1 - l_k, 1 \leq k \leq N\}$ . Simultaneously, since each Bob  $j$  ( $1 \leq j \leq N-1$ ) holds one qubit  $B_j$  and knows a part of complex part  $\varphi_j$ , so, the corresponding complete set of orthonormal basis can be expressed as

$$\begin{pmatrix} |v_0\rangle_{B_j} \\ |v_1\rangle_{B_j} \end{pmatrix} = V'^{(l_j)}(\varphi_j) \begin{pmatrix} |0\rangle_{B_j} \\ |1\rangle_{B_j} \end{pmatrix}, \quad (21)$$

where  $l_j$  represents the value of subscript in  $|u_{l_1 l_2 \dots l_N}\rangle$ ,  $l_j \in \{0, 1\}$ , and

$$V'^{(0)}(\varphi_j) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi_j} \\ 1 & -e^{-i\varphi_j} \end{pmatrix}, \quad (22)$$

$$V'^{(1)}(\varphi_j) = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\varphi_j} & 1 \\ -e^{-i\varphi_j} & 1 \end{pmatrix}. \quad (23)$$

### 3.2 Our $N$ -To-One JRSP protocol

By utilizing the measurement bases constructed in Sect. 3.1, we present an improved deterministic  $N$ -to-one JRSP of an arbitrary qubit as below.

**Prerequisite.** Suppose preparers (Alice, Bob 1, Bob 2, ... and Bob  $N-1$ ) want to help the receiver Charlie prepare an arbitrary single-qubit state (given in Eq. (1)), and they share  $N$  EPR pairs as quantum channel, which is described as

$$|Q\rangle_{A_1 B_1 A_2 B_2 \dots A_N C} = |EPR\rangle_{A_1 B_1} |EPR\rangle_{A_2 B_2} \dots |EPR\rangle_{A_{N-1} B_{N-1}} |EPR\rangle_{A_N C}, \quad (24)$$

Here, Alice is allowed to know  $\{a, b\}$ , Bob 1, Bob 2, ... and Bob  $N-1$  share the knowledge of  $\varphi$ , and each Bob  $j$  ( $1 \leq j \leq N-1$ ) knows  $\varphi_j$ , where  $\varphi = \sum_{j=1}^{N-1} \varphi_j$ .

**Step 1.** Alice measures her  $N$  qubits with the basis (given in Eq. (20)) and publicly broadcasts the measuring outcome  $l_1 l_2 \dots l_N$  ( $l_1, l_2, \dots, l_N \in \{0, 1\}$ ) to Bob 1, Bob 2, ... Bob  $N-1$  and Charlie.

**Step 2.** Each Bob  $j$  independently measures her qubit  $B_j$  in the basis conditioned on  $\varphi_j$  and Alice's outcome  $l_j$ . Specifically, each Bob  $j$  uses a basic measurement shown in Eq. (21). After measurement, each Bob  $j$  announces her measurement outcome  $m_j$  ( $m_j \in \{0, 1\}$ ) to Charlie.

**Step 3.** Charlie converts the qubit  $C$  to be the desired state  $|\phi\rangle_C$  by applying reconstruction operators  $R_{\underbrace{l_1 l_2 \dots l_N}_N \underbrace{m_1 m_2 \dots m_{N-1}}_{N-1}} = Z^{\underbrace{l_N \oplus m_1 \oplus m_2 \oplus \dots \oplus m_{N-1}}_{N-1}}$

$$X^{\underbrace{l_1 \oplus l_2 \oplus \dots \oplus l_N}_N}.$$



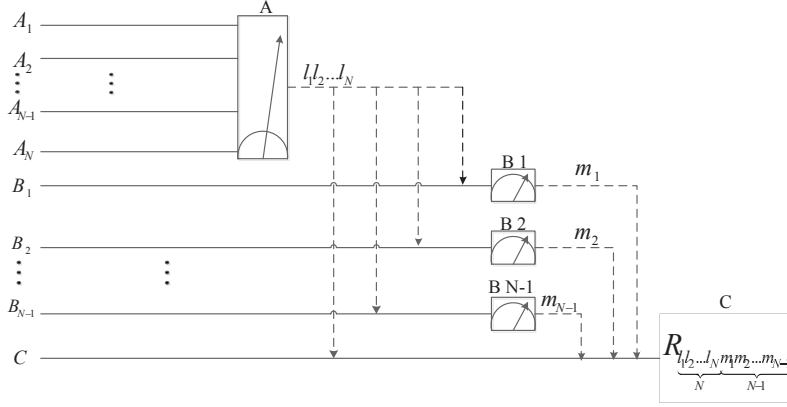


Fig. 2: The quantum circuit for deterministic deterministic  $N$ -to-one JRSP of an arbitrary qubit via  $N$  EPR pairs. Particles  $A_1 A_2 \dots A_N$  are hold by Alice,  $B_1, B_2, \dots, B_{N-1}$  hold by Bob 1, Bob 2,  $\dots$  and Bob  $N-1$ , respectively, and  $C$  hold by Charlie. The classical communications are represented as the dashed arrows, while the quantum channels are represented as the solid lines. what is more, boxes A, B1, B2, and B  $N-1$  depict Alice's, Bob 1's, Bob 2's,  $\dots$ , and Bob  $N-1$ 's measurement operation, respectively, and the last box  $C$  denotes the unitary operation Charlie carries out.

The whole process of our  $N$ -to-one JRSP protocol can also be described in a quantum circuit form as shown in Fig. 2. For clarity, we consider  $N = 3$  (Alice, Bob 1, Bob 2) as example, and  $|Q\rangle_{A_1 B_1 A_2 B_2 A_3 C} = |EPR\rangle_{A_1 B_1} |EPR\rangle_{A_2 B_2} |EPR\rangle_{A_3 C}$  is the quantum channel. At first, Alice measures her three qubits in the basis  $\{|u_{l_1 l_2 l_3}\rangle_{A_1 A_2 A_3}; l_1, l_2, l_3 \in \{0, 1\}\}$ :

$$\begin{pmatrix} |u_{000}\rangle_{A_1 A_2 A_3} \\ |u_{001}\rangle_{A_1 A_2 A_3} \\ |u_{010}\rangle_{A_1 A_2 A_3} \\ |u_{011}\rangle_{A_1 A_2 A_3} \\ |u_{100}\rangle_{A_1 A_2 A_3} \\ |u_{101}\rangle_{A_1 A_2 A_3} \\ |u_{110}\rangle_{A_1 A_2 A_3} \\ |u_{111}\rangle_{A_1 A_2 A_3} \end{pmatrix} = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & a & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & a & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & a & b & 0 & 0 & 0 \\ 0 & 0 & 0 & -b & a & b & 0 & 0 \\ 0 & 0 & -b & 0 & 0 & a & 0 & 0 \\ 0 & -b & 0 & 0 & 0 & 0 & a & 0 \\ -b & 0 & 0 & 0 & 0 & 0 & 0 & a \end{pmatrix} \begin{pmatrix} |000\rangle_{A_1 A_2 A_3} \\ |001\rangle_{A_1 A_2 A_3} \\ |010\rangle_{A_1 A_2 A_3} \\ |011\rangle_{A_1 A_2 A_3} \\ |100\rangle_{A_1 A_2 A_3} \\ |101\rangle_{A_1 A_2 A_3} \\ |110\rangle_{A_1 A_2 A_3} \\ |111\rangle_{A_1 A_2 A_3} \end{pmatrix}, \quad (25)$$

and publicly broadcasts outcome  $l_1 l_2 l_3$ . Before measurement, the quantum channel can be rewritten as

$$|Q\rangle_{A_1 B_1 A_2 B_2 A_3 C} = \frac{1}{2\sqrt{2}} \sum_{l_1=0}^1 \sum_{l_2=0}^1 \sum_{l_3=0}^1 |u_{l_1 l_2 l_3}\rangle_{A_1 A_2 A_3} |L_{l_1 l_2 l_3}\rangle_{B_1 B_2 C}. \quad (26)$$

And we derive  $|L_{l_1 l_2 l_3}\rangle_{B_1 B_2 C}$  in the form

$$|L_{l_1 l_2 l_3}\rangle_{B_1 B_2 C} = a |l_1 l_2 l_3\rangle_{B_1 B_2 C} + (-1)^{l_1} b \overline{|l_1 l_2 l_3\rangle}_{B_1 B_2 C}. \quad (27)$$

After Alice's measurement, Bob 1 and Bob 2 use the basis to measure their own qubit. The state in Eq. (27) can be expressed as

$$|L_{l_1 l_2 l_3}\rangle_{B_1 B_2 C} = \frac{1}{2} \sum_{m_1=1}^2 \sum_{m_2=1}^2 |v_{m_1}\rangle_{B_1} |v_{m_2}\rangle_{B_2} |\phi\rangle_C. \quad (28)$$

We assume  $l_1 l_2 l_3 = 010$  without generality, then Bob 1 and Bob 2 choose the basis  $\{|v_{m_1}\rangle_{B_1} |m_1 \in \{0, 1\}\}$

$$\begin{pmatrix} |v_0\rangle_{B_1} \\ |v_1\rangle_{B_1} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi_1} \\ 1 & -e^{-i\varphi_1} \end{pmatrix} \begin{pmatrix} |0\rangle_{B_1} \\ |1\rangle_{B_1} \end{pmatrix}, \quad (29)$$

and  $\{|v_{m_2}\rangle_{B_2} |m_2 \in \{0, 1\}\}$ :

$$\begin{pmatrix} |v_0\rangle_{B_2} \\ |v_1\rangle_{B_2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\varphi_2} & 1 \\ -e^{-i\varphi_2} & 1 \end{pmatrix} \begin{pmatrix} |0\rangle_{B_2} \\ |1\rangle_{B_2} \end{pmatrix}, \quad (30)$$

respectively. We can rewritten  $|L_{010}\rangle_{B_1 B_2 C}$  as

$$\begin{aligned} |L_{010}\rangle_{B_1 B_2 C} &= \frac{1}{2} a (|v_0\rangle_{B_1} + |v_1\rangle_{B_1}) (|v_0\rangle_{B_2} + |v_1\rangle_{B_2}) |0\rangle_C \\ &\quad + \frac{1}{2} b e^{i(\varphi_1 + \varphi_2)} (|v_0\rangle_{B_1} - |v_1\rangle_{B_1}) (|v_0\rangle_{B_2} - |v_1\rangle_{B_2}) |1\rangle_C \\ &= \frac{1}{2} |v_0\rangle_{B_1} |v_0\rangle_{B_2} (a|0\rangle + b e^{i(\varphi_1 + \varphi_2)} |1\rangle)_C \\ &\quad + \frac{1}{2} |v_0\rangle_{B_1} |v_1\rangle_{B_2} (a|0\rangle - b e^{i(\varphi_1 + \varphi_2)} |1\rangle)_C \\ &\quad + \frac{1}{2} |v_1\rangle_{B_1} |v_0\rangle_{B_2} (a|0\rangle - b e^{i(\varphi_1 + \varphi_2)} |1\rangle)_C \\ &\quad + \frac{1}{2} |v_1\rangle_{B_1} |v_1\rangle_{B_2} (a|0\rangle + b e^{i(\varphi_1 + \varphi_2)} |1\rangle)_C. \end{aligned} \quad (31)$$

Easy to see, whatever the outcome is, Charlie can achieve the desirable state by applying some reconstruction unitary operator  $R_{l_1 l_2 l_3 m_1 m_2}$  (all of which are shown in Table 2), and the success probability in each cases is 1. Moreover, the probability of obtaining the state  $|L_{l_1 l_2 l_3}\rangle_{B_1 B_2 C}$  for each of the outcomes  $\{l_1 l_2 l_3\}$  is equal. So, the total success probability  $P_{suc}^{N \geq 2}$  can be calculated as below

$$P_{suc}^{N \geq 2} = \left(\frac{1}{8} \times 1\right) \times 8 = 1. \quad (32)$$

## 4 Summary

In this paper, through analyzing Bich et al.'s second protocol with  $N > 2$  preparers, we find that the success probability  $P_{suc}^{N > 2} = 1/4 < 1$ . In order to fix the drawback, we firstly constructed two sets of projective measurement bases: the real-coefficient basis  $\{|u_{l_1 l_2 \dots l_N}\rangle |l_k \in \{0, 1\}\}$  and the complex-coefficient basis  $\{|v_0\rangle_{B_j}, |v_1\rangle_{B_j}\}$ , and further proposed an improved deterministic  $N$ -to-one

Table 2: The collapsed state  $|\phi\rangle_C$  of Charlie's qubits  $C$  and the corresponding recovery operators  $R_{l_1 l_2 l_3 m_1 m_2}$  related to the measurement outcomes  $(l_1 l_2 l_3, m_1, m_2)$  from Alice, Bob 1 and Bob 2

$l_1 l_2 l_3$	$m_1 m_2$	$ \phi\rangle_C$	$R_{l_1 l_2 l_3 m_1 m_2}$
000	00	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
	01	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	10	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	11	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
001	00	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
	01	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	10	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	11	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
010	00	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
	01	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	10	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	11	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
011	00	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
	01	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	10	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	11	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
100	00	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
	01	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	10	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	11	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
101	00	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
	01	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	10	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	11	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
110	00	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
	01	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	10	$a 0\rangle - be^{i(\varphi_1+\varphi_2)} 1\rangle$	$Z$
	11	$a 0\rangle + be^{i(\varphi_1+\varphi_2)} 1\rangle$	$I$
111	00	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$
	01	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	10	$a 1\rangle - be^{i(\varphi_1+\varphi_2)} 0\rangle$	$ZX$
	11	$a 1\rangle + be^{i(\varphi_1+\varphi_2)} 0\rangle$	$X$

JRSP protocol for an arbitrary single-qubit state with unit success probability (i.e,  $P_{suc}^{N \geq 2} = 1$ ).

In addition, our protocol is also flexible and convenient: depending on the need, we can assign a receiver after sharing the quantum channel and the receiver may not be sufficiently well equipped. What is more, based on

our protocol, we can structure a practical network: Alice can be regarded as a Service Provider, she just distributes EPR pairs and measures her qubits; Other participants (Bob 1, Bob 2, ..., Bob N-1 and Charlie) can be regarded as customers, while one of them is a receiver and the others are preparers. That is to say, with the help of Alice, arbitrary customer can be a receiver or preparer.

**Acknowledgements** This work is supported by the National Nature Science Foundation of China (Grant Nos. 61103235, 61170321, 61373016 and 61373131), the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), the State Key Laboratory of Software Engineering, Wuhan University (SKLSE2012-09-41), and the Practice Innovation Training Program Projects for the Jiangsu College Students (201310300018Z).

## References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984, 175-179. IEEE Press, New York (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* 68(21), 3121-3124 (1992).
3. Yang, J., Xu, B.J., Guo, H.: Source monitoring for continuous-variable quantum key distribution. *Phys. Rev. A* 86(4), 042314 (2012). doi:10.1103/PhysRevA.86.042314
4. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. *Phys. Rev. Lett.* 83(3), 648-651 (1999). doi:10.1103/PhysRevLett.83.648
5. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. *Phys. Rev. A* 59(3), 1829-1834 (1999). doi:10.1103/PhysRevA.59.1829
6. Wang, H. B.; Huang, Y. G.; Fang, X.; Gu, B.; Fu, D. S.: High-capacity three-party quantum secret sharing with single photons in both the polarization and the spatial-mode degrees of freedom. *Int. J. Theor. Phys.* 52(4), 1043-1051 (2013). doi:10.1007/s10773-012-1418-x
7. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* 68(4), 042317 (2003). doi:10.1103/PhysRevA.68.042317
8. Liu, W.J., Chen, H.W., Li, Z.Q., Liu, Z.H.: Efficient quantum secure direct communication with authentication. *Chin. Phys. Lett.* 25(7), 2354-2357 (2008).
9. Liu, W.J., Chen, H.W., Ma, T.H., Li, Z.Q., Liu, Z.H., Hu, W.B.: An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication. *Chinese Phys. B* 18(10), 4105-4109 (2009). doi:10.1088/1674-1056/18/10/007
10. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* 70(13), 1895-1899 (1993).
11. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. *Nature* 390(6660), 575-579 (1997). doi:10.1038/37539
12. Long, L.R., Li, H.W., Zhou, P., Fan, C., Yin, C.L.: Multiparty-controlled teleportation of an arbitrary GHZ-class state by using a d-dimensional (N+2)-particle nonmaximally entangled state as the quantum channel. *Sci. China. Phys. Mech.* 54(3), 484-490 (2011). doi:10.1007/s11433-011-4246
13. Liu, W.J., Liu, C., Liu, Z.H., Liu, J.F., Geng, H.T.: Same Initial States Attack in Yang et al.'s Quantum Private Comparison Protocol and the Improvement. *Int. J. Theor. Phys.* 53(1), 271-276 (2013).
14. Liu, W.J., Liu, C., Wang, H.B., Jia, T.T.: Quantum Private Comparison: A Review. *IETE Tech. Rev.* 30(5), 439-445 (2013). doi:10.1007/s10773-013-1807-9
15. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. *Sci. China. Phys. Mech.* 56(9), 1670-1678 (2013). doi:10.1007/s11433-013-5224-0

16. Pati, A.K.: Minimum classical bit for remote preparation and measurement of a qubit. *Phys. Rev. A* 63(1), 014302 (2000).
17. Bennett, C.H., DiVincenzo, D.P., Shor, P.W., Smolin, J.A., Terhal, B.M., Wootters, W.K.: Remote State Preparation. *Phys. Rev. Lett.* 87(7), 077902 (2001).
18. Lo, H.-K.: Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. *Phys. Rev. A* 62(1), 012313 (2000).
19. Xia, Y., Song, J., Song, H.S.: Multiparty remote state preparation. *J. Phys. B: At. Mol. Opt. Phys.* 40(18), 3719-3724 (2007). doi:10.1088/0953-4075/40/18/011
20. An, N.B., Kim, J.: COLLECTIVE REMOTE STATE PREPARATION. *Int. J. Quantum Inf.* 6(5), 1051-1066 (2008). doi:10.1142/s0219749908004304
21. Chen, Q.Q., Xia, Y., Song, J., Nguyen, B.A.: Joint remote state preparation of a W-type state via W-type states. *Phys. Lett. A* 374(44), 4483-4487 (2010). doi:10.1016/j.physleta.2010.09.013
22. Luo, M.X., Chen, X.B., Ma, S.Y., Niu, X.X., Yang, Y.X.: Joint remote preparation of an arbitrary three-qubit state. *Opt. Commun.* 283(23), 4796-4801 (2010). doi:10.1016/j.optcom.2010.07.043
23. Nguyen, B.A.: Joint remote preparation of a general two-qubit state. *J. Phys. B: At. Mol. Opt. Phys.* 42(12), 125501 (2009). doi:10.1088/0953-4075/42/12/125501
24. Nguyen, B.A.: Joint remote state preparation via W and W-type states. *Opt. Commun.* 283(20), 4113-4117 (2010). doi:10.1016/j.optcom.2010.06.016
25. Xia, Y., Song, J., Song, H.S., Guo, J.L.: MULTIPARTY REMOTE STATE PREPARATION WITH LINEAR OPTICAL ELEMENTS. *Int. J. Quantum Inf.* 6(5), 1127-1134 (2008). doi:10.1142/s0219749908004328
26. Xiao, X.-Q., Liu, J.-M., Zeng, G.: Joint remote state preparation of arbitrary two-and three-qubit states. *J. Phys. B: At. Mol. Opt. Phys.* 44(7), 075501 (2011).
27. An, N.B., Bich, C.T., Van Don, N.: Deterministic joint remote state preparation. *Phys. Lett. A* 375(41), 3570-3573 (2011). doi:10.1016/j.physleta.2011.08.045
28. Xia, Y., Chen, Q.-Q., An, N.B.: Deterministic joint remote preparation of an arbitrary three-qubit state via EinsteinCPodolskyCRosen pairs with a passive receiver. *J. Phys. A: Math. Theor.* 45(33), 335306 (2012).
29. Yuan, W., Xin, J.: Deterministic joint remote state preparation of arbitrary two-and three-qubit states. *Chinese. Phys. B* 22(2), 020306 (2013).
30. Ming-Ming, W., Xiu-Bo, C., Yi-Xian, Y.: Deterministic Joint Remote Preparation of an Arbitrary Two-Qubit State Using the Cluster State. *Commun. Theor. Phys.* 59(5), 568 (2013).
31. Bich, C.T., Don, N.V., An, N.B.: Deterministic Joint Remote Preparation of an Arbitrary Qubit via Einstein-Podolsky-Rosen Pairs. *Int. J. Theor. Phys.* 51(7), 2272-2281 (2012). doi:10.1007/s10773-012-1107-9
32. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, (2010)
33. Segal, I.E.: Postulates for general quantum mechanics. *The Annals of Mathematics* 48(4), 930-948 (1947).